IEEE P802.11
Wireless LANs

|  |
| --- |
| Use Case for Rogue Detection |
| Date: 2019-11-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java DrSunnyvale, CA | +1-303-818-8472 | mark.hamilton2152@gmail.com |
|  |  |  |  |  |

Abstract

Propose replacing the “rogue containment” use case in the RCM TIG report with a “rogue detection” use case.

**Discussion**:

The use case “Rogue containment in infrastructure networks” has raised concerns that the containment action portion of the use case may be illegal or otherwise constrained in some juridictions. Since the containment actions are not really relevant to the randomized MAC address concepts, they can be removed from the use case with no loss of relevance to the discussion in the TIG’s report.

**Proposal**:

Direct the editor to replace the “Rogue containment in infrastructure networks” with the following use case, 3.8, in the group report:

# Use-cases

RCM TIG has explored different use-cases that are impacted by the expected future prevalence of randomized and changing MAC addresses in .11 networks.

# Rogue detection in infrastructure networks

A managed WLAN network may desire to detect rogue, un-authorised access points and/or client stations operating in its service area. One such rogue detection mechanism entails monitoring for users associated to access points which which are not known to be part of the managed network. The MAC addresses of the known APs are kept in a database, and the medium is monitored for Beacons or other broadcast traffic from, or non-AP STAs’ traffic to, APs not on the known AP list.

Non-AP STAs could also be listed on a known client list, by MAC address, and thereby unexpected/unwanted client devices in the service area can be detected, by detecting unknown MAC addresses.

When a rogue AP or STA is detected, appropriate action (such as contacting the owner) can be taken to resolve any issues such as interference with the operation of the managed WLAN.

# Local-ID MAC address impacts

APs which use a randomized MAC address, expecially likely with mobile APs for example, could be difficult to identify and take appropriate corrective action. Similarly, detection of rogue non-AP STAs would become difficult.

Even known and desired non-AP STAs will not be able to be detected via MAC address capture and filtering, thus causing “false alarms” of rogue client detections.

# Rapidly changing MAC address impacts

The faster the speed of change the more difficult to detect and/or track down rogue devices, so rapidly changing MAC addresses makes the above issues worse.